

פתרון תרגיל בית 5 בתורת החבורות 88-218 סמסטר א' תש"ף

שאלה 1 (חימום). תארו את כל המחלקות השמאליות ב- $\mathbb{Z}_{30}/\langle 3 \rangle$. פתרון. האיבר 3 הוא מסדר 10, ולכן $|\langle 3 \rangle| = 10$. לפי משפט לגראנז' נקבל

$$|\mathbb{Z}_{30}/\langle 3 \rangle| = \frac{|\mathbb{Z}_{30}|}{|\langle 3 \rangle|} = \frac{30}{10} = 3$$

והמחלקות, עד כדי בחירת נציגים, הן $\{\langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$.

שאלה 2. מצאו את האינדקסים הבאים:

א. $[U_{14} : \langle 11 \rangle]$ רמז: משפט לגראנז'.

ב. $[\mathbb{Z}_8 \times \mathbb{Z}_8 : \langle (2, 2) \rangle]$ רמז: משפט לגראנז'.

ג. $[\mathbb{Z} \times \mathbb{Z} : \langle (2, 2) \rangle]$ רמז: קודם תארו את המחלקות השמאליות.

פתרון.

א. איברי U_{14} הם הטבעיים שקטנים וזרים ל-14. כלומר $U_{14} = \{1, 3, 5, 9, 11, 13\}$. חישוב קצר יראה כי $\langle 11 \rangle = \{1, 9, 11\}$, ואז לפי משפט לגראנז' נקבל שיש בדיוק שתי מחלקות שמאליות. כלומר $[U_{14} : \langle 11 \rangle] = 2$.

ב. הסדר של החבורה $\mathbb{Z}_8 \times \mathbb{Z}_8$ הוא $8 \cdot 8 = 64$, והסדר של תת-החבורה $\langle (2, 2) \rangle$ הוא כסדר של האיבר $(2, 2)$, שהוא 4. לכן לפי משפט לגראנז' $[\mathbb{Z}_8 \times \mathbb{Z}_8 : \langle (2, 2) \rangle] = 64/4 = 16$.

ג. נוכיח כי $[\mathbb{Z} \times \mathbb{Z} : \langle (2, 2) \rangle] = \infty$ לפי זה שנראה ש- $\{(0, n) + \mathbb{Z} \times \mathbb{Z}\}$ היא קבוצה אינסופית של מחלקות שמאליות שונות (אלו לא כל המחלקות). אם $(0, n) + \mathbb{Z} \times \mathbb{Z} = (0, m) + \mathbb{Z} \times \mathbb{Z}$ זה אומר

$$(0, n) - (0, m) \in \langle (2, 2) \rangle$$

כלומר ש- $(0, n - m) = (2k, 2k)$ לאיזשהו $k \in \mathbb{Z}$. לכן $0 = n - m$, ולכן $n = m$. כלומר יש אינסוף מחלקות שמאליות שונות.

שאלה 3. תהי G חבורה ותהינה $H, K \leq G$ תת-חבורות סופיות שלה.

א. הוכיחו שאם $(|H|, |K|) = 1$, אז $H \cap K = \{e\}$.

ב. יהי p מספר ראשוני. הוכיחו שאם $|H| = |K| = p$ וגם $H \neq K$, אז $H \cap K = \{e\}$.

פתרון.

א. ידוע לנו כי $H \cap K$ היא תת־חבורה של H ושל K . לכן לפי משפט לגראנז' מתקיים כי $|H \cap K|$ מחלק את $|H|$ ואת $|K|$. אך לפי הנתון הממ"מ של $|H|$ ו- $|K|$ הוא 1. לכן $|H \cap K| \leq 1$. אבל תמיד $|H \cap K| \geq 1$ כי איבר היחידה שייך אליו, ולכן קיבלנו כי $H \cap K = \{e\}$.

ב. יהי $x \in H \cap K$ איבר כלשהו. נניח בשלילה כי $x \neq e$. לכן $o(x) > 1$. אנחנו יודעים כי $o(x)$ מחלק את $|H|$ ואת $|K|$, ולכן בהכרח $o(x) = p$. כלומר $|\langle x \rangle| = p$ ומפני ש- H, K הן חבורות אז הן סגורה לפעולה ונסיק $\langle x \rangle \subseteq H, K$. מהנתון $|H| = |K| = p$ נקבל $H = K = \langle x \rangle$ כי ב- $\langle x \rangle$ יש בדיוק p איברים שונים. אך זו סתירה לנתון, ונסיק כי $x = e$.

שאלה 4. יהי p ראשוני, ותהי G חבורה מסדר p^3 .

א. הוכיחו שניתן ליצור את G עם תת־קבוצה בת שלושה איברים $a, b, c \in G$ (כלומר $G = \langle a, b, c \rangle$). רמז: משפט לגראנז' כמה וכמה פעמים.

ב. בחרו p . תנו דוגמה מפורשת לחבורה G אבלית מסדר p^3 שאפשר ליצור עם שני איברים $a, b \in G$, אבל לא עם איבר אחד.

ג. רשות: הראו שישנה חבורה לא אבלית מסדר p^3 שאפשר ליצור עם שני איברים לפי ההדרכה הבאה: התבוננו בקבוצה (שכבר פגשנו מעל \mathbb{R})

$$H(\mathbb{Z}_p) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{Z}_p \right\}$$

ועל האיברים $a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. הראו כי $p^2 = |\langle a, aba^{-1}b^{-1} \rangle|$, והסיקו מזה ש- $H(\mathbb{Z}_p) = \langle a, b \rangle$.

פתרון.

א. כמסקנה ממשפט לגראנז' אנחנו יודעים שהסדרים האפשריים של איברים ב- G הם $\{1, p, p^2, p^3\}$. אם קיים איבר $a \in G$ מסדר p^3 , אז G ציקלית ומתקיים $G = \langle a \rangle$. לכן נוכל לבחור **כל** זוג איברים $b, c \in G$ ויתקיים

$$G = \langle a \rangle \leq \langle a, b, c \rangle \leq G$$

כלומר $G = \langle a, b, c \rangle$.

אם לא קיים איבר מסדר p^3 , אבל קיים איבר $a \in G$ מסדר p^2 , אבל תת־חבורה $\langle a \rangle$ מכילה p^2 איברים. לכן קיים איבר $b \in G \setminus \langle a \rangle$ והסדר שלו הוא לפחות p . לכן

$$|\langle a, b \rangle| \geq |\langle a \rangle \cup \{b\}| > |\langle a \rangle| = p^2$$

כי $b \notin \langle a \rangle$. אבל הסדר של $\langle a, b \rangle$ חייב לחלק את p^3 , ולכן הוא בדיוק p^3 . כך נוכל לבחור כל איבר נוסף $c \in G$ ונקבל

$$G = \langle a, b \rangle \leq \langle a, b, c \rangle \leq G$$

ושוב נקבל $G = \langle a, b, c \rangle$.

אם לא קיימים איברים מסדר p^3 או p^2 , אז הסדר של כל האיברים הוא p , פרט לאיבר היחידה. יהי $a \in G$ איבר מסדר p . אז $|\langle a \rangle| = p$. נבחר $e \neq b \in G \setminus \langle a \rangle$. אז לפי לגראנז' הסדר של תת־חבורה $\langle a, b \rangle$ מחלק את $|G| = p^3$, ובנוסף הוא חייב להיות גדול מ- p , כי $|\langle a \rangle \cup \{b\}| = p + 1$. לכן $|\langle a, b \rangle| \geq p^2$. אם $|\langle a, b \rangle| = p^3$, נסיים כמו מקודם. אחרת, $|\langle a, b \rangle| = p^2$ ונוכל לבחור $e \neq c \in G \setminus \langle a, b \rangle$ מסדר p ומטיעון דומה נסיק $G = \langle a, b, c \rangle$.

ב. עד כדי איזומורפיזם, אפשר לבחור רק את $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$. למשל עבור $p = 2$ נבחר את $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, ואת האיברים $a = (1, 0)$, $b = (1, 1)$. זה מתאים למקרה השני של הסעיף הקודם, שבו אין איבר מסדר p^3 , אבל $o(a) = p^2$ ובחרנו את $b \neq (0, 0)$ כך ש- $b \notin \langle a \rangle$.

ג. ברור שחבורה לא אבלית לא ניתן ליצור עם איבר אחד. לפי ההדרכה נחשב כי $aba^{-1}b^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (הוא גם איבר מסדר p). הכפל בחבורה מקיים

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & xy'+z+z' \\ 0 & 1 & y+y' \\ 0 & 0 & 1 \end{pmatrix}$$

בתת-החבורה $\langle a, aba^{-1}b^{-1} \rangle$ ליוצרים יש במיקום $(2, 3)$ רכיב 0, ולכן באינדוקציה לכל איבר בתת-החבורה יש 0 במיקום $(2, 3)$ (הראו שתת-החבורה איזומורפית ל- $(\mathbb{Z}_p \times \mathbb{Z}_p)$). אזי $\langle a, aba^{-1}b^{-1} \rangle$ אינו מכיל $b \notin \langle a, aba^{-1}b^{-1} \rangle$ ולפי הסעיף הראשון נסיק שהיא מסדר p^3 . אבל $\langle a, aba^{-1}b^{-1} \rangle \subseteq \langle a, b \rangle$ ולכן a, b יוצרים את $H(\mathbb{Z}_p)$.

שאלה 5. הוכיחו שלכל $n, s > 1$ מתקיים כי $n | \varphi(s^n - 1)$. המספר $\varphi(s^n - 1)$ הוא סדר של חבורה מוכרת.

פתרון. לפי הרמז נשים לב כי $|U_{s^n-1}| = \varphi(s^n - 1)$. אם נמצא איבר $x \in U_{s^n-1}$ מסדר n , אז נסיים לפי מסקנה ממשפט לגראנז' שבה מראים כי סדר של איבר מחלק את סדר החבורה.

נבחר את $x = s$. קל לבדוק כי $(s^n - 1) \cdot (s - 1) \cdot s^{n-1} = 1$ ולכן $(s, s^n - 1) = 1$. כלומר $s \in U_{s^n-1}$. נותר להראות שהסדר של s בחבורה הוא n . תחילה להיתכנות, מחשבים

$$s^n \equiv 1 \pmod{s^n - 1}$$

ולכן $n | \varphi(s^n - 1)$. למינימליות של הסדר, נשים לב כי $s^i < s^n - 1$ לכל $i < n$ כמספרים טבעיים. לכן גם בהכרח s^i אינו שקול ל-1 מודולו $s^n - 1$. בסך הכל $\varphi(s^n - 1) = n | \varphi(s^n - 1)$.

שאלה 6. מצאו את כל המספרים n כך ש- $\varphi(n) = 4$ וכל המספרים m כך ש- $\varphi(m) = 8$. זה בסדר להשתמש במחשב עבור פעולות חשבון פשוטות.

פתרון. אם ראשוני $p \geq 7$ מחלק את n , אז $\varphi(n) > 4$. לכן מחפשים מספרים מהצורה $n = 2^a 3^b 5^c$ עם הדרישות $a < 4$, $b < 2$, $c < 2$. בדיקה זריזה אחרי פתרונות בקבוצה הסופית הזאת למשוואה $\varphi(n) = 4$ תגלה שהם רק 5, 8, 10, 12.

באופן דומה, אם ראשוני $p \geq 11$ מחלק את m , אז $\varphi(m) > 8$. לכן מחפשים מספרים מהצורה $m = 2^a 3^b 5^c 7^d$ עם הדרישות $a < 5$, $b < 3$, $c < 2$, $d < 2$. בדיקה זריזה אחרי פתרונות בקבוצה הסופית הזאת למשוואה $\varphi(m) = 8$ תגלה שהם רק 15, 16, 20, 24, 30.

שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרם אותן, בבקשה שלחו לנו את הפתרון שלהן.

שאלה 7. תהי G חבורה. נגדיר את המעריך של החבורה $\exp(G)$ (או האקספוננט) להיות המספר הטבעי הקטן ביותר n כך שלכל $g \in G$ מתקיים $g^n = e$. אם לא קיים כזה, נאמר $\exp(G) = \infty$.

כתבו תוכנה המחשבת את כל הסדרים האפשריים ב- S_n ואת $\exp(S_n)$. זה בסדר להשתמש במערכות תוכנה מתמטיות כמו SageMath.

שאלה 8. תהי I קבוצה מכוונת (כלומר I היא קבוצה סדורה חלקית כך שלכל $i, j \in I$ קיים $k \in I$ כך ש- $k > i, j$). מערכת של חבורות $\{G_i\}_{i \in I}$ נקראת רשת עולה אם לכל $i < j$ מתקיים $G_i \subseteq G_j$.
הוכיחו שבמקרה זה $\bigcup_{i \in I} G_i$ היא חבורה. בפרט, אם ישנה שרשרת עולה של חבורות $G_1 \subseteq G_2 \subseteq \dots$, אז גם איחוד השרשרת הוא חבורה.

בהצלחה!